PCT/ SE 00 / 0 1 4 0 7
10/019491

SE00/1407

PRV

PATENT- OCH REGISTRERINGSVERKET
Patentavdelningen

Intyg
Certificate

Härmed intygas att bifogade kopior överensstämmer med de handlingar som ursprungligen ingivits till Patent- och registreringsverket i nedannämnda ansökan.

This is to certify that the annexed is a true copy of the documents as originally filed with the Patent- and Registration Office in connection with the following patent application.

(71) *Sökande* / *Applicant (s)* — *Sike & Co, Jönköping SE*

(21) *Patentansökningsnummer* / *Patent application number* — *9902532-2*

(86) *Ingivningsdatum* / *Date of filing* — *1999-07-01*

Stockholm, 2000-08-24

För Patent- och registreringsverket
For the Patent- and Registration Office

Åsa Dahlberg

Åsa Dahlberg

Avgift
Fee

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

PATENT- OCH REGISTRERINGSVERKET
SWEDEN

Postadress/Adress
Box 5055
S-102 42 STOCKHOLM

Telefon/Phone
+46 8 782 25 00
Vx 08-782 25 00

Telex
17978
PATOREG S

Telefax
+46 8 666 02 86
08-666 02 86

Apparatus and method for safeguarding electronic equipment from theft

Technical field of the invention

The invention relates to an apparatus and a method for preventing electronic equipment from theft.

Background of the invention

Current industrial as well as private investments in computerised equipment and electronic devices grow rapidly and these investments form property of considerable value to the owners. However, this valuable property also attracts people to commit criminal acts and in illegal ways lay their hands on items belonging to others.

Not only the so-called hardware i.e. interconnected electronic circuits with memories and displays, but also and perhaps even more vulnerable may be so-called software and content of various memory locations of the electronic devices. Occurrence of sensitive data or material stored in a memory location of e.g. a laptop computer in wrong hands may have severe consequences to any company or to a private person if this content is made public.

Several mechanical means for prevention computer thefts are offered on the market, especially for preventing people from stealing stationary desktop computers in offices. Those means may be for example metallic safety lockers or wires, which physically hinders people from opening or carrying the computer with them. Such physical means mostly are expensive, cumbersome to install and not at all flexible. However, for mobile equipment like for instance portable laptop computers, even less practical theft-preventing means are offered on the market. Most prior art safeguarding arrangements are software encryption systems, which are very useful al-

though the electronic components do not lose their value after theft from the legitimate owner.

The UK patent application GB 2 304 810 A discloses a security arrangement with sensors detecting light levels inside of a persona computer housing or motion of the personal computer. Furthermore, the arrangement inside the computer consists of a dye capsule, which is intended to rupture and spray its content outwardly upon reception of an electrical signal. This signal is sent from an alarm output control when the personal computer is considered stolen. It is of course difficult to distinguish usual "every day" handling of the personal computer in reliable manners from unauthorised handling after that the computer has been stolen. Conceivable when such an implemented security arrangement would be numerous false alarms leading to strongly decreased acceptance of the arrangement.

Summary of the invention

An object of the present invention is to overcome the aforementioned drawbacks concerning prior art technology in connection with stationary and portable computers as well as with electronic devices and circuitry in general.

The above mentioned object of the invention is accomplished by an apparatus for safeguarding electronic equipment. The equipment is provided in housing, comprising monitoring means, such as a sensor arrangement, to monitor whether the housing in closed or not and/or whether an authorised person operates the electronic equipment. Furthermore it can be characterised by destruction initiation means connected to and controlled by the monitoring means. Preferably is comprises at least one destruction means provided in connection with the electronic equipment and particularly chosen to get the electronic equipment irreversibly out of order when initiated by the destruction initiation means.

Suitably, a remote control means is in connection with the monitoring means and/or with the destruction initiation means to feed a simulation signal simulating an im-

proper operation of the electronic equipment by an unauthorised person at remote control.

A housing sensor means would be convenient, sensing if the housing is unauthorised opened, whereby the housing sensor means is adapted to send a warning signal to the monitoring means when sensing unauthorised opening. In another embodiment, conceivable would be to use electronic equipment sensing means sensing unauthorised disconnection of at least one component in the electronic equipment, whereby the electronic equipment is adapted to send a warning signal to the monitoring means when detecting unauthorised disconnection.

The apparatus moreover comprises identification means, identifying a user and possibly authorising the user after comparison with a register, whereby the electronic equipment could be unlocked. Said identification means either comprises a so-called smart card reading means, operating with physical contacting or without physical contacting and/or a PIN-code reading means and/or any other human feature recognising means, such as a fingerprint recogniser.

In order to guarantee provision of energy for running the safeguarding apparatus, autonomous power supplying means such as a battery may be provided, supplying the apparatus and its parts with electric power after having been disconnected from a mains power outlet.

Suitably, said destruction means generates a pulse of high voltage and/or current, which is lead through electronic circuitry, whereby essential components within the circuitry are irreversibly set out of order. Else, said destruction means could generate a destructive injection, preferably of a highly conductive and/or corroding chemical fluid, which is distributed over essential electronic components, whereby the components are irreversibly set out of order.

For enhanced flexibility, remote control means could be useful, by which remote signals from a remote control station can be received, whereby actions can be taken by the safeguarding apparatus in response to sent remote signals.

To notify potential thieves about the apparatus installed, application of at least one visible label on the outside of the electronic equipment would be of great help for calling people's attention to the safeguarding apparatus.

Furthermore, prior art is afflicted with problems that are solved by a method for safeguarding electronic equipment, which equipment is provided in housing. The housing comprises monitoring means, such as a sensor arrangement, to monitor whether the housing in closed or not and/or whether an authorised person operates the electronic equipment. The method is characterised by connecting and controlling the destruction initiation means by the monitoring means and providing at least one destruction means in the electronic equipment particularly chosen to set the electronic equipment irreversibly of order when initiated by the destruction initiation means.

Owing to the present invention as here described, a novel approach is presented that offers the market a convenient and cheap apparatus and method inhibiting incentives for stealing computer-related devices. The present invention will be referred to as Badger™ device and has the advantage that the trade-in value of electronic devices, possibly removed from stolen computers is diminished due to the irreversible damage caused to the devices.

Brief description of the drawings

The present invention will now be discussed in more detail with reference to preferred embodiments of the present invention, given only by way of example, and illustrated in the accompanying drawings, in which:

Fig 1 shows a schematic block diagram of one embodiment of the safeguarding apparatus in accordance with the present invention,

Fig 2 illustrates in a block diagram the sequence from indication to destruction of electronic devices of the electronic equipment.

Detailed description

With reference to Fig 1 showing a block diagram of a first embodiment of the present invention for safeguarding electronic equipment 100, for example stationary or portable computers. A safeguarding apparatus 10, which in the following will be referred to either as Badger™ device 10 or apparatus 10, comprises a number of parts 20, 25, 30, 40, 45, 50 formed integrally with the apparatus 10 or in connection with it. One of these parts are for instance an identification unit 20, which utilises one state of the art identification procedure, such as smart card reading or PIN-code input by an operator or user. When identification is accomplished, the operator or user is compared with a register 25 of predefined authorised operators or users and may subsequently be authorised for usage of safeguarded electronic equipment 100. The identification process could also take advantage of other unique human features, conceivable would be fingerprint recognition or iris detection techniques.

Another part in connection with the apparatus 10 is an autonomous power supply 30, including a power management control function. The autonomous power supply preferably is a battery or other power-storing element. The apparatus 10 and its parts 20, 25, 30, 40, 45, 50 could normally be power supplied by the same mains power supply 115 as the electronic equipment 100. However, the apparatus 10 and its main parts could instead be power supplied only by the autonomous power supply 30. Alternatively there could be a switching device 31 automatically connecting the power supply 30 to the apparatus 10 and its parts as soon as a disruption of the mains supply 115 has occurred. The apparatus 10 thus can switch between the states "mains" and "soft" power supply. A switching device 31 of this kind is well known to a person skilled in the art and is therefore not shown in detail. If the apparatus 10 is disconnected from the mains power outlet 115, it automatically switches over to

"soft" power supply and at the same time the electronic equipment 100 changes its mode from "unlocked" to "locked" mode.

This means that the user or operator must identify himself to the identification means 20 in any of the above-described manners in order to unlock the electronic equipment 100. If this identification is not properly performed and the locked mode is forced in a violent way, the safeguard process is activated leading to an irreversible destruction of electronic components contained in the electronic equipment 100. However, this process will be further described in the following.

Furthermore, next part to be described, which part may be integrally designed or in connection with the apparatus 10, is a destruction initiating means 40. In one embodiment, this generating means 40 generates one for the electric circuitry excessively high voltage and/or high current, which is lead through the circuitry, preferably as reverse current through a diode, whereby essential electronic devices either melt or are otherwise irreversibly damaged and made useless. In another embodiment, destructive highly conductive or corrosive chemical fluid is stored within the electronic equipment 100, which fluid at control from the destruction initiating means 40 may be set free and thus can be distributed over essential components in the electronic equipment 100. Hereby is achieved a similar way of destruction of essential components either through short-circuiting electrical circuitry or corroding vital components instead of melting as in the first embodiment. Also a combination of the above-mentioned techniques would be a possible and fruitful approach.

Next part to be described shown in Fig 1 is a remote control equipment comprising a transceiver 50, which comprises at least a receiver but preferably also a transmitter. By means of the receiver, remote signals can be received from a remote control station 120, which station may be any kind of wireless interfaced transceiver means, such as a mobile telephone or infrared communication terminal, enabling a way of remote accessibility to the safeguarding apparatus 10. In one embodiment including an outward transmitter it is possible to confirm destructive actions taken by the gen-

erating means 40 back to the remote control station 120, whereby a legitimate user or operator can be informed about the destructive actions that recently have been performed.

Still with reference to Fig 1, the output 14 of the safeguarding apparatus 10 in bi-directional connection with the input 101 of the electronic equipment 100, suitably via a communication bus 92. The same output 14 or another output 12 of the safeguarding apparatus 10 is in bi-directional connection with an input 111 of a sensor arrangement 110 via communication bus 94. The monitoring sensor arrangement 110 monitors the operation of the electronic devices 102, 104, 106, 108 of the electronic equipment and the position of the housing of the electronic equipment 100. Should damage be caused upon the housing, or the housing be opened in any unauthorised way, the safeguarding apparatus 10, via the generating means 40, takes the necessary steps to irreversibly setting the electronic devices out of order. In one embodiment, these destructive actions are taken via inputs 103, 105, 107, 109 of a motherboard 102, plug-in cards 104, drives 106 and read/write memory locations 108 respectively.

Yet another part in connection with the electronic equipment 100 is a characteristic label 60 placed on the outside of the housing of the safeguarded equipment 100. The label 60 does not show any direct technical operative functionality but may be of great importance to the safeguarding apparatus 10 anyway. Electronic equipment 100 marked with the label 60 at least indicates a considerable additional difficulty in selling stolen electronic devices, originally belonging to the electronic equipment 100, already before the actual theft was done. This because of the fact that the devices will be destroyed and substantially lack trade-in value. For that reason, the label 60 is of great importance in strengthening the safeguard of the apparatus 10.

Referring to Fig 2, which is a schematic block diagram showing sequentially the steps for irreversible destruction of electronic devices contained in the electronic equipment 100. In one embodiment an indication is forwarded to the Badger™ de-

vice 10 from the monitoring sensor arrangement 110, which indication results from for instance unauthorised opening of the housing of the electronic equipment 100 (step 1a). In another embodiment, this indication can be transmitted (step 1b) from a remote control station 120, such as a telephone or an infrared communication terminal. However, a receiver in connection with the safeguarding apparatus 10 must receive the remote signal. In both of the above cases, the apparatus 10 instructs (step 2) a destruction means 45, preferably a pulse generator, to generate a destructive pulse (step 3) with an output power sufficient for irreversible destruction of the electronic devices of the equipment 100. Feedback in form of a confirming signal message is suitably sent from the pulse generator 45 or from the safeguard apparatus 10 to the remote communication terminal 120 from which the destructive instructions initially was sent. However, in that case a transmitter in connection with the safeguarding apparatus 10 must send the remote confirmation signal. The destructive pulse generated in step 3 by the destruction means 40, 45 is forwarded to of the electronic devices to be irreversibly set out of order (step 4), preferably at least one of the following devices, motherboard 102, plug-in cards 104, drives 106 and read/write memory locations 108.

The destruction means 45 could for example be a conductor from the destruction initiating means 40 connected to a leg of an integrated circuit known to be vulnerable and sensitive for a destruction pulse.

Claims

1. An apparatus for safeguarding electronic equipment (100) provided in a housing, comprising monitoring means (110), such as a sensor arrangement, to monitor whether the housing in closed or not and/or whether the electronic equipment is operated by an authorised person,

characterised by

destruction initiation means (40) connected to and controlled by the monitoring means (110);

at least one destruction means (45) provided in connection with the electronic equipment (100) particularly chosen to get the electronic equipment (110) irreversibly out of order when initiated by the destruction initiation means (40).

2. An apparatus according to claim 1, **characterised by**

remote control means (50) in connection with the monitoring means (110) and/or with the destruction initiation means (40) to feed a simulation signal simulating an improper operation of the electronic equipment (100) by an unauthorised person at remote control.

3. An apparatus according to claim 1 or 2, **characterised by**

housing sensor means (200) sensing if the housing is unauthorised opened, whereby the housing sensor means (200) is adapted to send a warning signal to the monitoring means (110) when sensing unauthorised opening.

4. An apparatus according to anyone of the claims 1-3, **characterised by**

electronic equipment sensing means (201) sensing unauthorised disconnection of at least one component in the electronic equipment (100), whereby the electronic equipment (100) is adapted to send a warning signal to the monitoring means (110) when detecting unauthorised disconnection.

5. An apparatus according to anyone of the preceding claims, **characterised by** identification means (20), identifying a user and possibly authorising the user after comparison with a register (25), whereby the electronic equipment (100) could be unlocked.

6. An apparatus according to claim 5, **characterised in that** said identification means (20) either is a so-called smart card reading means, operating with physical contacting or without physical contacting or a PIN-code reading means or any other human feature recognising means, such as a fingerprint recogniser.

7. An apparatus according to anyone of the claims 1-4, **characterised by** autonomous power supplying means (30), such as a battery, supplying the apparatus (10) and its parts (20, 30, 40, 45, 50) with electric power after having been disconnected from a mains power outlet (115).

8. An apparatus according to anyone of the claims 1-4, **characterised in that** said destruction means (45) generates a pulse of high voltage and/or current, which is lead through electronic circuitry, whereby essential components within the circuitry are irreversibly set out of order.

9. An apparatus according to anyone of the claims 1-4, **characterised in that** said destruction means (45) generates a destructive injection, preferably of a highly conductive and/or corroding chemical fluid, which is distributed over essential electronic components, whereby the components are irreversibly set out of order.

10. An apparatus according to anyone of the claims 1-4, **characterised by** remote receiving control means (50), by which transmitted remote signals from a remote transmitting control station (120) are received, adapted to take actions, via the safeguarding apparatus (10), in response to the received remote signals.

11. Apparatus as claimed in anyone of the preceding claims, **characterised by**

application of at least one visible label (60) on the outside of the electronic equipment (100) for calling people's attention to the safeguarding apparatus (10) installed.

12. A method for safeguarding electronic equipment (100) provided in a housing, comprising monitoring means (110), such as a sensor arrangement, to monitor whether the housing in closed or not and/or whether the electronic equipment is operated by an authorised person,

characterised by

connecting and controlling the destruction initiation means (40) by the monitoring means (110);

providing at least one destruction means (45) in the electronic equipment (110) particularly chosen to set the electronic equipment (110) irreversibly of order when initiated by the destruction initiation means (40).

Abstract

The present invention relates to an apparatus and a method for safeguarding valuable electronic equipment (100) from theft. The safeguarding is connected to a monitoring means (110), monitoring whether an unauthorised person has opened a housing of the electronic equipment. An identification means (20) may authorise users. Unauthorised breaking of the housing results in generation by destruction means (40, 45) of an electric pulse fed through electronic devices (102, 104, 106, 108), whereby said devices are irreversibly set out of order and thus their trade-in value is considerably diminished.

Fig 1.

PRV 98-07-01

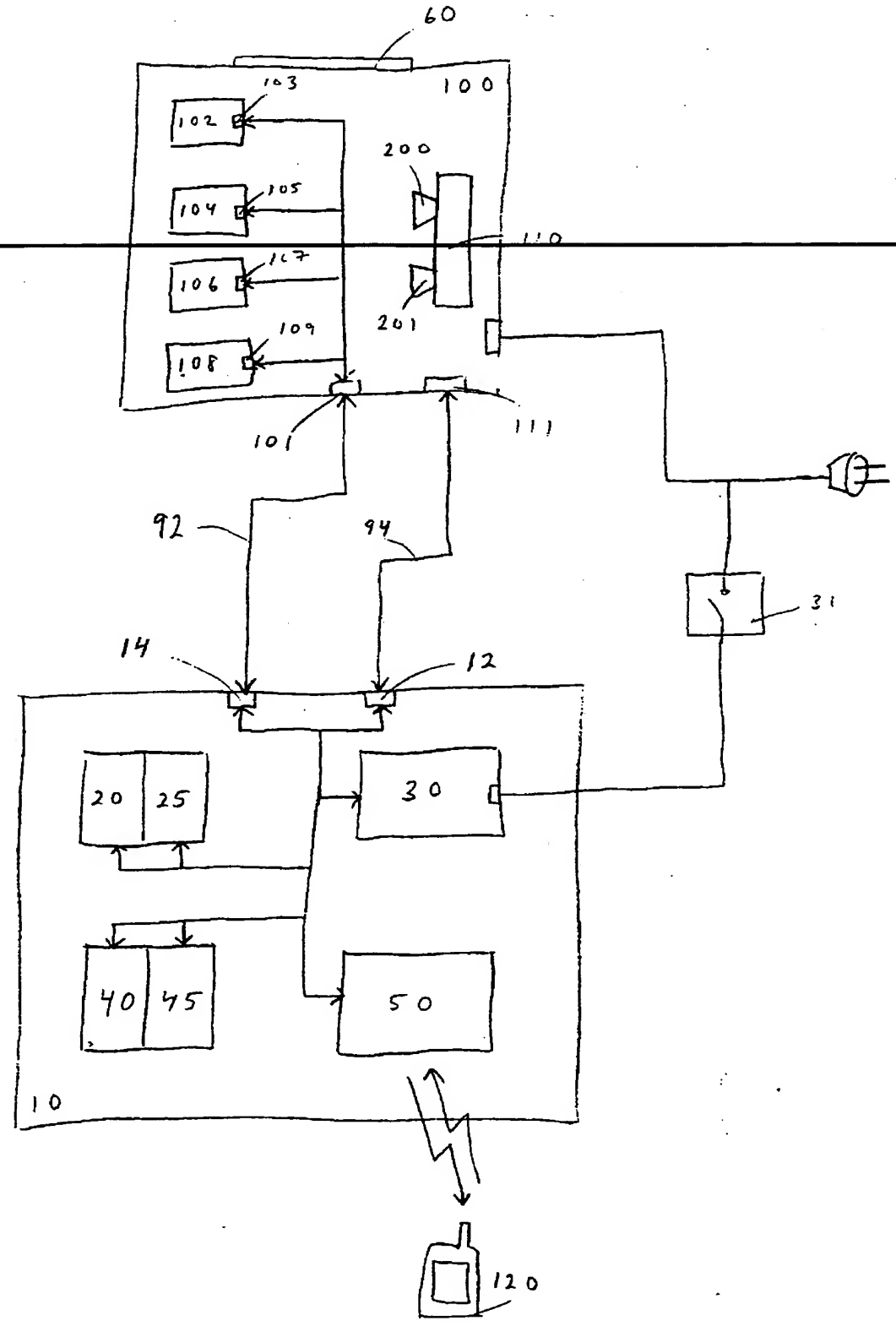
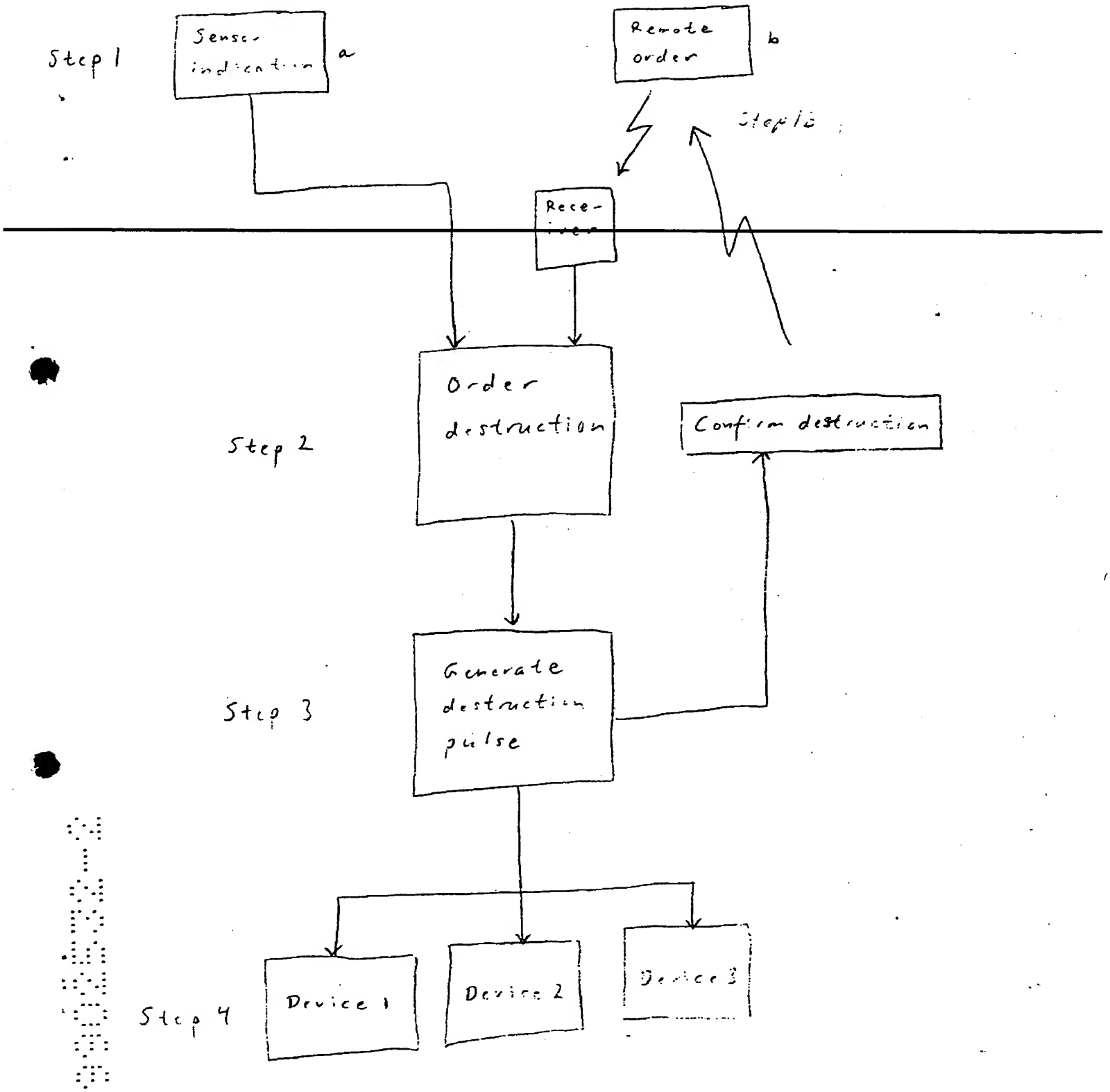


Fig 2.

PRV 98-07-01



This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☒ FADED TEXT OR DRAWING
- ☒ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☒ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.